UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/014,912	12/14/2001	Toshihisa Nakano	2001_1837A	4213

513 7590 04/21/2005

WENDEROTH, LIND & PONACK, L.L.P.
2033 K STREET N. W.
SUITE 800
WASHINGTON, DC 20006-1021

EXAMINER	
PARTHASARATHY, PRAMILA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 04/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/014,912	NAKANO ET AL.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12/01 2/02 10/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on 12/06/2001. Claims 1 – 20 were received for consideration. No preliminary amendments to the claims were filed. Claims 1 – 20 are currently being considered.

Information Disclosure Statement

2. Three initialed and dated copies of Applicant's IDS form 1449 are attached to the Office action.

Specification

3. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: Key Management Device For Copyright Protection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1 – 22 are rejected under 35 U.S.C. 102(e) as being anticipated by Itkis (U.S. Patent Number 6,880,081).

5. Regarding Claim 1, Itkis discloses key storage means for storing the keys, wherein each key is associated with a node one N-layer tree structure (N is 2 or a natural than 2) (Column 8 lines 8 – 34 and Column 9 lines 11 – 35), and

each key group includes keys associated with a different group nodes, each group of nodes being a set of nodes located on a different path, in each tree structure, connecting a different node on the N^{th} layer and a node on the highest layer (Column 8 lines 8 – 34 and Column 9 lines 11 – 35); and

encryption information generating means for, upon receipt information designating a key group assigned to one of the reproducing devices,

(1) invalidating each key in the designated key group (Column 9 lines 11 – 35 and Column 12 lines 35 – 53),

(2) selecting non-invalid keys being immediately subordinate to each invalid key from among keys in the key groups that are assigned to the other recording devices and/or the other reproducing devices and each of which includes one or more invalid keys (Column 9 lines 11 – 56 and Column 12 lines 35 – 53), and

3) generating encryption information that includes (i) at least one ciphertext corresponding to a content key that is used to encrypt the data, the ciphertexts being generated by encrypting the content key using each selected key (Column 9 line 49 – Column 10 line 14 and Column 12 lines 38 – 41), and

(ii) identification information for identifying the selected keys (Column 9 line 49 – Column 10 line 14); and

each reproducing device stores N keys assigned thereto, selectively decrypts one of the ciphertexts that is decryptable using a key identified by the identification information to obtain the content key, and decrypts the data using the thus obtained content key to reproduce a content (Column 8 lines 8 – 34; Column 9 lines 11 – 35 and Column 12 line 35 – Column 13 line 14).

6. Regarding Claim 12, discloses each key in the key group being assigned to a node forming an N-layer tree structure (N is 2 or a natural number greater than 2) together with nodes with which keys stored in the other reproducing devices are associated (Column 8 lines 8 – 34 and Column 9 lines 11 – 35),

the keys in the key group being associated with a group of nodes that is a set of nodes located on a path, in each tree structure, connecting a node on the N^{th} layer and a node on the highest layer (Column 8 lines 8 – 34 and Column 9 lines 11 – 35),

the recording medium comprising: a data area which stores data generated by encrypting a content using a content key (Column 3 lines 11 – 39 and Column 6 lines 42 – 59);

a ciphertext area which stores at least one ciphertext generated by encrypting the content key using a key being identical to one of the selected key, the selected keys stored in each reproducing device except for a specifically designated reproducing device (Column 3 lines 11 – 39 and Column 6 lines 42 – 59); and

a selected key list area which stores information identifying the selected key used for encrypting the content key (Column 12 lines 38 – 41 and Column 13 lines 5 – 24).

7. Regarding Claim 13, Itkis discloses key group storing means for storing N keys (N is 2 natural number greater than 2) (Column 8 lines 8 – 34 and Column 9 lines 11 – 35), wherein

the N keys are respectively associated with nodes forming an N-layer tree structure together with nodes with which keys stored in other reproducing devices are associated, and the N keys are associated with a group of nodes that is a set of nodes located on a path, in the tree structure, connecting a node on the Nth layer to a node on the highest layer (Column 8 lines 8 – 34 and Column 9 lines 11 – 35);

reproduction information obtaining means for obtaining

(i) the data by encrypting a content using a content key, (ii) at least one ciphertext generated by encrypting the content key, and (iii) identification information for identifying a key used to encrypt the content key (Column 9 line 57 – Column 10 line 13 and Column 12 line 60 – Column 13 line 14);

content key decrypting means for selecting a key identified by the identification information from the keys stored in the key group storage means, and decrypting the

ciphertext that is decryptable using the thus selected key to obtain the content key (Column 8 lines 8 – 34; Column 9 lines 11 – 35 and Column 12 line 60 – Column 13 line 14);

and content reproducing means for decrypting the data using the thus obtained content key reproduce the content (Column 12 line 35 – 64).

8. Regarding Claims 16, 17 and 18, Itkis discloses the keys are grouped into a plurality of key groups each of which is assigned to one of a plurality of reproducing devices, each key is associated with a node forming at least one N-layer tree structure (N is 2 or a natural number greater than 2) (Column 8 lines 8 – 34 and Column 9 lines 11 – 35),

each key group includes keys associated with a different group of nodes, each group of nodes being set of nodes located on a different path, each tree structure, connecting a different node on the N^{th} layer and a node on the highest layer (Column 8 lines 8 – 34 and Column 9 lines 11 – 35), the key management method comprising:

an accepting step for accepting information designating a key group stored in one of the reproducing devices;

a key selecting step for

(1) invalidating each key in the designated key group (Column 9 lines 11 – 35 and Column 12 lines 35 – 53),

(2) selecting non-invalid keys being immediately subordinate to each invalid key from among keys in the key groups that are assigned to the other recording devices

and/or the other reproducing devices and each of which includes one or more invalid keys (Column 9 lines 11 – 56 and Column 12 lines 35 – 53), and

3) generating encryption information that includes (i) at least one ciphertext corresponding to a content key that is used to encrypt the data, the ciphertexts being generated by encrypting the content key using each selected key (Column 9 line 49 – Column 10 line 14 and Column 12 lines 38 – 41), and

(ii) identification information for identifying the selected keys (Column 9 line 49 – Column 10 line 14); and wherein

each reproducing device stores N keys assigned thereto, selectively decrypts one of the ciphertexts that is decryptable using a key identified by the identification information to obtain the content key, and decrypts the data using the thus obtained content key to reproduce a content (Column 8 lines 8 – 34; Column 9 lines 11 – 35 and Column 12 line 60 – Column 13 line 14).

9. Regarding Claim 19, Itkis discloses a system comprising:

a plurality of recording devices for recording encrypted data to a rewritable recording medium (Column 3 lines 11 – 39 and Column 6 lines 42 – 59);

a plurality of reproducing devices for decrypting and reproducing the encrypted data being recoded in the recording medium (Column 3 lines 11 – 39 and Column 6 lines 42 – 59); and

a key management device for managing keys, the keys being grouped into a plurality of key groups each of which is assigned to the plurality reproducing devices,

wherein the key management device includes (Column 3 lines 11 – 39 and Column 6 lines 42 – 59);

key storage means storing the keys, wherein each key is associated with a node forming at least one N-layer tree structure (N is 2 or a natural number greater than 2) (Column 8 lines 8 – 34 and Column 9 lines 11 – 35), and

each key group includes keys associated with a different group of nodes, each group of nodes being a set of nodes located on a different path, in each tree structure, connecting a different node on the N^{th} layer and a node on the highest layer (Column 8 lines 8 – 34 and Column 9 lines 11 – 35);

encryption information generating means for, upon receipt of information designating a key group assigned to one of the recording devices and/or one the reproducing devices,

(1) invalidating each key in the designated key group (Column 9 lines 11 – 35 and Column 12 lines 35 – 53),

(2) selecting non-invalid keys being immediately subordinate to each invalid key from among keys in the key groups that are assigned to the other recording devices and/or the other reproducing devices and each of which includes one or more invalid keys (Column 9 lines 11 – 56 and Column 12 lines 35 – 53), and

3) generating encryption information that includes (i) at least one ciphertext corresponding to a content key that is used to encrypt the data, the ciphertexts being generated by encrypting the content key using each selected key (Column 9 line 49 – Column 10 line 14 and Column 12 lines 38 – 41), and

(ii) identification information for identifying the selected keys (Column 9 line 49 – Column 10 line 14); and

encryption information recording means for recording the thus generated encryption information to the recording medium (Column 9 line 49 – Column 10 line 14 and Column 12 lines 35 - 41),

each recording device includes :

key group storing means for storing N keys, the N keys being associated with nodes located on a path, in each tree structure, connecting a node on the N^{th} layer to a node on the highest layer (Column 8 lines 8 – 34 and Column 9 lines 11 – 35);

content key decrypting means for reading the encryption information from the recording medium, identifying a key stored in the key group storing means using the identification information, and decrypting the ciphertext being decryptable with the thus identified key to obtain the content key (Column 8 lines 8 – 34; Column 9 lines 11 – 35 and Column 12 line 60 – Column 13 line 14); and

content encrypting means for encrypting a content using the thus obtained content key, and record the resulting encrypted data to the recording medium, and each reproducing device includes :

key group storing means for storing N keys, the N keys being associated With nodes located on a path, in the tree structure, connecting a node on the N^{th} layer to a node on the highest layer (Column 8 lines 8 – 34; Column 9 lines 11 – 35 and Column 12 line 60 – Column 13 line 14);

reproduction information obtaining means for obtaining the data generated by encrypting the content using the content key, the ciphertext generated by encrypting the content key, and the identification information for identifying the key used to encrypt the content key (Column 9 line 57 – Column 10 line 13 and Column 12 line 60 – Column 13 line 14);

content key decrypting means for selecting a key identified by the identification information from the keys stored in the key group storage means, and decrypting the ciphertext decryptable using the thus selected key to obtain the content key (Column 8 lines 8 – 34; Column 9 lines 11 – 35 and Column 12 line 60 – Column 13 line 14); and

content reproducing means for decrypting the data using the thus obtained content key to reproduce the content (Column 12 line 35 – 64).

10. Regarding Claim 20, Itkis discloses the key groups together include keys each of which is associated with a node forming an N-layer tree structure (N is a natural number greater than 2) (Column 8 lines 8 – 34 and Column 9 lines 11 – 35),

each key group includes keys associated with of nodes that is a set of different group of nodes, each group nodes located on a different path, in the tree structure, connecting a different node on the N^{th} layer and a node on the highest layer (Column 8 lines 8 – 34 and Column 9 lines 11 – 35),

the recording medium comprising:

a ciphertext area for storing at least one ciphertext generated by encrypting the content key using a selected key, the selected key being identical to a key stored in the

recoding device and key stored in the reproducing device (Column 3 lines 11 – 39 and Column 6 lines 42 – 59);

a selected key area for storing identification information identifying the selected key used for encrypting the content key (Column 12 lines 38 – 41 and Column 13 lines 5 – 24); and

a data area for storing data recorded by the recording device, the data being decryptable using the content key, the content key is obtained by decrypting the ciphertext using the key that is stored in the reproducing device and selected according to the identification information (Column 3 lines 11 – 39 and Column 6 lines 42 – 59).

11. Regarding Claim 21, Itkis discloses key storing means key storage means for storing the keys, wherein each key is associated with a node one N-layer tree structure (N is 2 or a natural than 2) (Column 8 lines 8 – 34 and Column 9 lines 11 – 35), and

each key group includes keys associated with a different group nodes, each group of nodes being a set of nodes located on a different path, in each tree structure, connecting a different node on the N^{th} layer and a node on the highest layer (Column 8 lines 8 – 34 and Column 9 lines 11 – 35); and

encryption information generating means for, upon receipt information designating a key group assigned to one of the reproducing devices,

(1) invalidating each key in the designated key group (Column 9 lines 11 – 35 and Column 12 lines 35 – 53),

(2) selecting non-invalid keys being immediately subordinate to each invalid key from among keys in the key groups that are assigned to the other recording devices and/or the other reproducing devices and each of which includes one or more invalid keys (Column 9 lines 11 – 56 and Column 12 lines 35 – 53), and

3) generating encryption information that includes (i) at least one ciphertext corresponding to a content key that is used to encrypt the data, the ciphertexts being generated by encrypting the content key using each selected key (Column 9 line 49 – Column 10 line 14 and Column 12 lines 38 – 41), and
(ii) identification information for identifying the selected keys (Column 9 line 49 – Column 10 line 14); and

encryption information recording means f or recording the thus generated encryption information to the recording medium (Column 9 line 49 – Column 10 line 14 and Column 12 lines 35 - 41).

12. Regarding Claim 22, Itkis discloses key group storing means for storing N keys (N is 2 or a natural number greater than 2) (Column 8 lines 8 – 34 and Column 9 lines 11 – 35), wherein

the N keys are respectively associated with nodes forming an N-layer tree structure together with nodes with which keys stored in other recording devices are associated (Column 8 lines 8 – 34 and Column 9 lines 11 – 35), and

the N keys are associated with a group of nodes that is a set of nodes located on a path, in the tree structure, connecting a node on the N^{th} layer to a node on the highest layer (Column 8 lines 8 – 34 and Column 9 lines 11 – 35);

content key decrypting means for reading the encryption information from the recording medium, selecting a key stored in the key group storing means using identification information, and decrypting a ciphertext being decryptable with the thus selected key to obtain the content key, wherein the recording medium pre-stores encryption information including at least the ciphertext encrypted using the selected key and the identification information for identifying the selected key (Column 8 lines 8 – 34; Column 9 lines 11 – 35 and Column 12 line 60 – Column 13 line 14); and

content encrypting means for encrypting a content using the thus obtained content key, and record the resulting encrypted data the recording medium (Column 12 line 35 – 64).

13. Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Itkis discloses data generating unit which generates the data by encrypting the content using the content key;

an invalid key accepting unit which accepts the information designating the key group assigned to the one reproducing device (Column 3 lines 11 – 39 and Column 6 lines 42 – 59);

key selecting unit which invalidates each key in the designated key group, and selects the non-invalid keys being immediately subordinate on a different path to each

invalid key except for the invalid key residing on the N^{th} layer (Column 3 lines 11 – 39 and Column 6 lines 42 – 59);

a ciphertext generating unit which generates the ciphertexts by encrypting the content key using each selected key (Column 3 lines 11 – 39 and Column 6 lines 42 – 59); and

a selected key list generating unit which generates a list used to identify the selected keys (Column 12 lines 38 – 41 and Column 13 lines 5 – 24).

14. Claim 11 is rejected as applied above in rejecting claim 1. Furthermore, Itkis discloses the key storage means stores L tree structures, L being 2^{k+1} when the maximum number of key groups to be invalidated is set at 2^k (Column 8 lines 8 – 34 and Column 9 lines 11 – 35).

15. Claims 14 and 15 are rejected as applied above in rejecting claim 13. Furthermore, Itkis discloses i) the data generated by encrypting the content using the content key, (ii) the ciphertext generated by encrypting the content key, and (iii) the information for identifying the key used to decrypt the content key, and passing the read result to the reproduction information obtaining means (Column 8 lines 8 – 34; Column 9 lines 11 – 35 and Column 12 line 60 – Column 13 line 14).

16. Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, Itkis discloses the key storage means includes a key management information storage unit

which stores each key's (i) identifier for identifying the key, (ii) parent key identifier for identifying its parent key being immediately superordinate to the key, (iii) key state information showing whether the key is a selected key being used to generate one of the ciphertexts, an invalid key, or a non-used key, and key data (Column 12 lines 35 – 53), and

the invalid key accepting unit accepts identifiers for each key in the designated key group, and the key selecting unit

(1) updates the key state information so as invalidate a key of which identifier matches any of the designated identifiers , and (2) updates the key state information so as to select a key (i) of which identifier does not match any of the designated identifiers, (ii) of which parent key is invalidated, and (iii) that is neither invalided nor selected (Column 6 lines 11 – 59, Column 9 lines 11 – 35 and Column 12 lines 35 – 53).

17. Claim 5 is rejected as applied above in rejecting claim 4. Furthermore, Itkis discloses a restoring key accepting unit which accepts information designating a key group that has been invalidated and to be restored and,

restoring unit which

(a) selects, from among the keys in the designated key group to be restored, key of which parent key being immediately superordinate to the key and a brother key having the same parent key are both invalidated (Column 9 lines 23 – 35), and

(b) changes a subordinate key of the thus selected key in the designated key group to a non-used key (Column 9 lines 23 – 56).

18. Claim 7 is rejected as applied above in rejecting claim 2. Furthermore, Itkis discloses new key accepting means for accepting the number of reproducing devices to which a key group is newly assigned;

new key generating means for generating keys which are associated with nodes forming an M-layer tree structure (M is a natural number between 2 and N inclusive) (Column 8 lines 8 – 34 and Column 9 lines 11 – 35); and

connecting means for replacing a key on the highest layer of the newly generated tree structure with a selected key or a non-used key residing on the $(N-M+1)^{th}$ or higher layer of the existing tree structure stored in the key recording means (Column 8 lines 8 – 34 and Column 9 lines 11 – 35).

19. Claim 8 is rejected as applied above in rejecting claim 2. Furthermore, Itkis discloses recording means for recording to a recording medium the data generated by the data generating unit, the ciphertexts generated by the ciphertext generating unit, and the selected key list generated by the selected key generating unit (Column 12 lines 38 – 41 and Column 13 lines 5 – 24).

20. Claim 9 is rejected as applied above in rejecting claim 2. Furthermore, Itkis discloses transmitting means for transmitting the plurality the data generating reproducing devices the data generated by unit, the ciphertexts generated by the ciphertext generating unit, and the selected key list generated by the selected key generating unit (Column 12 lines 38 – 41 and Column 13 lines 5 – 24).

21. Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Itkis discloses the key on the highest layer has a specific value as its parent key identifier, and the key selecting unit selects the key of which parent identifier has the specific value as a selected key unless the key is invalidated (Column 12 lines 38 – 41 and Column 13 lines 5 – 24).

22. Claim 10 is rejected as applied above in rejecting claim 3. Furthermore, Itkis discloses the key management information storing unit stores the key management information every time it is updated by the key selecting unit, and

the key storage means further includes a restoring unit for restoring the key management information back to its initial version or any updated version (Column 11 lines 10 – 57).

23. Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Itkis discloses the key storage means includes a key management information storage unit which stores, each key's (i) identifier for identifying the key, (ii) parent key identifier for identifying its parent key being immediately superordinate to the key, (iii) key state information showing whether the key is a selected key being used to generate one of the ciphertexts, an invalid key, or a non-used key, and key data (Column 12 lines 35 – 53),

the restoring key accepting unit accepts identifiers for each key in the designated key group be restored, and the restoring unit updates the key state information so

as select, from among keys having an identifier that matches any of the designated identifiers, (i) the key on the highest layer when its immediately subordinate key residing on a different path is currently selected, or (ii) a key on the second layer or below when its brother key having the same parent key is all invalidated (Column 9 lines 23 – 35),

change non-used key a key having an identifier that matches any of the designated identifiers and being subordinate on the same path to the thus selected key, and change non-used key a key having an identifier that does not match any of the designated identifiers and having the thus selected key as its parent key (Column 9 lines 23 – 35).

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
April 16, 2005.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100